I value teaching as highly as doing cutting-edge research and not because I have to, but because I actually do feel this way. I have a history of creating and teaching innovative and immersive classes in systems, currently focused on topics in computer security and operating systems. I have developed and actively teach courses in memory forensics, malware analysis, reverse engineering, digital forensics, advanced network security, offensive computing, operating systems internals, blockchain technologies, and darknets/anonymizing overlay networks. My expectation is that I could offer courses from this portfolio essentially on-demand. In the past, I’ve also taught courses in fault tolerant distributed systems, mobile computing, and computer graphics. My teaching experience spans many decades and I have experience teaching not only in a university setting, but also in intensive training scenarios in the corporate, intelligence, and and law enforcement communities.

I incorporate my research extensively into virtually every course I teach, at every level (undergraduate and graduate). This allows students to see the relevance of the material they’re tackling, provides abundant opportunities for students to contribute their ideas, and fosters interesting in-class discussion. In many cases, my own research projects spawn smaller projects that are appropriate for laboratory assignments or semester projects and these very often prove useful in the context of the larger research effort.

My teaching style involves providing students with foundational knowledge and then immersing them in real problems, offering as much guidance as necessary for them to solve the problems on their own. For example, in my malware reverse engineering course, students are immediately immersed in the dissection of complex malware samples, even though they may be (and often are) deficient in operating systems internals and assembly language skills. These and other skills, such as the intuition necessary for effective static and dynamic analysis, are then developed "on the job". After students submit their best-effort solutions, the entire class participates in an interactive walkthrough of my fully worked solution, which reinforces things the students got right in their own analyses, and fills in any remaining gaps in their understanding.

The graduate level memory forensics course I’ve recently developed is one of the first in the country and focuses on an emerging area in digital forensics that targets volatile application and operating systems data to extract actionable forensic evidence. This course briefly surveys historical aspects of memory forensics and then concentrates on using and improving popular memory forensics frameworks such as Volatility and Rekall. Students are necessarily exposed to a wide variety of systems-related topics in this course, including Windows, Mac, and Linux internals, malware detection and mitigation, and forensic analysis of closed source applications, making the course a great source for discovering and formulating research topics for M.S. and Ph.D. work.

I consider the thousands of students I’ve trained to be my most valuable contribution to society and I hope to continue teaching for many years to come.